IN THE SPECIFICATION

Please replace the paragraph beginning at page 7, line 14, with the following rewritten paragraph:

a1

In such ecommerce scenario, each customer has a private/public key pair, with the private key safely stored and used in a smart card, and registers the public key with many different ecommerce sites. Thus, the private/public key pair is used for many purposes. When the private key is compromised, the customer must prevent use of the private/public key pair at all ecommerce sites where the customer has registered the public key, and just remembering these sites could be a difficult task for the customer. Thus, there is a need for a new ~~mechansim~~ mechanism which allows the customer to prevent further use of the private/public key pair at all sites by taking a single action.

Please replace the paragraph beginning at page 13, line 21, with the following rewritten paragraph:

a2

Credentials server 42 is an on-line component of certificate authority 32 and is responsible for issuing the short-term disposable certificates and for maintaining the list of cryptographic hashes of currently valid unsigned certificates in hash table 44. Each cryptographic hash in hash table 44 is computed from an unsigned certificate using an agreed upon collision-resistant hash function, such as SHA-1 or MD5. Hash table 44 is essentially a list of the currently valid unsigned certificates which is keyed by the cryptographic hash. Cryptographic hashes function well as keys for hash table 44, because cryptographic hashes behave ~~statically~~ statistically as random quantities.

Please replace the paragraph beginning at page 25, line 5, with the following rewritten paragraph:

a3

The present invention concerns a user of a public key cryptosystem referred to as a subject (e.g., a human or a computer system), which has a public/private key pair, and which uses the key pair to demonstrate its identity to another user of the same cryptosystem referred to as a verifier. The subject uses a public key validation service (PKVS) to validate the subject's public key before using the key pair for authentication purposes, in such a way that

A3 con't

the public key will cease to be usable for authentication purposes if the subjects notifies the PKVS that the private key has been compromised.

Please replace the paragraph beginning at page 29, line 14, with the following rewritten paragraph:

A4

Credentials server 703 is an on-line component of PKVA 701 and is responsible for issuing the disposable certificates and for maintaining the list of cryptographic hashes of currently valid unsigned certificates in hash table 704. Each cryptographic hash in hash table 704 is computed from an unsigned certificate using an agreed upon collision-resistant hash function, such as SHA-1 or MD5. Hash table 704 is essentially a list of the currently valid unsigned certificates which is keyed by the cryptographic hash. Cryptographic hashes function well as keys for hash table 704, because cryptographic hashes behave ~~statically~~ statistically as random quantities.

Please replace the paragraph beginning at page 33, line 15, with the following rewritten paragraph:

A5

4. Certificate authority 705 creates and signs a revocable certificate 1000 and sends the revocable certificate to subject 706. Revocable certificate 1000 is illustrated in Figure 4 16 and comprises: a field 1001 containing a serial number; an optional field 1002 containing the subject's public key (obtained from field 801 of the unsigned PKVC 800); a field 1003 containing the one or more identity attributes sent in step 1 of Protocol P4; a field 1004 containing the PKVH computed in step 3 of Protocol P4; and a field 1005 containing an expiration date/time. In one embodiment, if the X.509v3 format is used, the field 1004 is flagged as being critical, to ensure that it will not be ignored by a older verifier that does not understand the purpose of this field. The revocable certificate 1000 also includes a signature field 1006 containing a digital signature computed over a sequence of non-signature fields 1007, such as fields 1001, 1002, 1003, 1004, and 1005, using the private key of certificate authority 705. The field 1002 is optional because the revocable certificate 1000 is used in conjunction with a disposable PKVC 900 that contains the

Amt 5

subject's public key and the PKVH 1004 is ~~derived from~~ associated with the subject's public key.

Please replace the paragraph beginning at page 35, line 17, with the following rewritten paragraph:

Amt 6

In authentication with disposable certificates as described above for Lightweight PKI 30/30' Employing Disposable Certificates, the certificate authority has an off-line component, the registration authority and an on-line component, the credentials server. The subject registers its public key and identity attributes with the registration authority. The registration authority issues an unsigned certificate to the subject, which binds the public key to the attributes, and sends the cryptographic hash of the unsigned certificate to the credentials server, which stores the cryptographic ~~has~~ hash in a hash table. Later, the subject submits the unsigned certificate to the credentials server and obtains a disposable certificate as long as the hash of the unsigned certificate is still in the hash table. Finally, the subject uses the disposable certificate, as well as knowledge of its private key, to demonstrate its identity to a verifier.

Please replace the paragraph beginning at page 35, line 29, with the following rewritten paragraph:

To take advantage of a PKVA, the above authentication method using disposable certificates is modified as follows. When registering with the registration authority of the regular certificate authority, the subject submits the unsigned PKVC and the public key of the PKVA instead of simply submitting its public key. The subject also submits its identity attributes as before. The registration authority issues a regular unsigned certificate to the subject ~~that binds~~ for binding the subject's ~~pubic~~ public key to the attributes. The registration authority sends to the credentials server a cryptographic hash computed by applying a collision-resistant hash function, such as MD5 and SHA-1, to the concatenation of the regular unsigned certificate with the PKVN and the public key of the PKVA. The credentials server adds the cryptographic hash to its hash table as before.

Please replace the paragraph beginning at page 36, line 9, with the following rewritten paragraph:

Later the subject submits the regular unsigned certificate to the credentials server of the regular certificate authority, together with a disposable PKVC and the public key of the PKVA. The credentials server uses the public key of the PKVA to verify the signature on the disposable PKVC. If the regular unsigned certificate includes an optional filed containing the subject's public key, ~~The~~ the credentials server checks that the public key appearing in the regular unsigned certificate is the same public key that appears in the disposable PKVC. The credentials server computes a cryptographic hash by applying the same collision-resistant hash function to the concatenation of the regular unsigned certificate, the PKVN contained in the PKVC, and the public key of the PKVA, and checks that the cryptographic hash appears in its hash table. If the computed cryptographic hash appears in the credentials server's hash table, the credentials server issues to the subject a regular disposable certificate that binds the public key of the subject to the identity attributes. The disposable PKVC must still be valid, and the expiration date/time of the regular disposable certificate is set so that it will expire no later than the disposable PKVC. As in the above unmodified authentication method using disposable certificates, the subject uses the regular disposable certificate, as well as knowledge of its private key, to demonstrate its identity to a verifier.

Please ~~replace~~ the paragraph beginning at page 37, line 1, with the following rewritten paragraph:

If the private key is compromised, the subject notifies the PKVA, which revokes the unsigned PKVC. After the PKVA revokes the unsigned PKVC, the PKVA will no longer issue disposable PKVCs binding the public key of the subject to the same PKVN. Therefore, an attacker cannot obtain regular disposable certificates from the credentials server based on the previously-issued regular unsigned certificate. The attacker can register the subject's public key with the same PKVA or with a different PKVA and obtain a disposable PKVC for the public key. The attacker can then submit the subject's regular unsigned certificate, the disposable PKVC, and the public key of the PKVA, to the credentials server. However, the hash computed by the credentials server will not match the hash that was sent by the registration authority to the credentials server when the subject registered with the

Q7 amt

registration authority. Indeed, if the attacker has used a different PKVA, the public key of the PKVA used in the hash computation will be different. If the attacker has used the same PKVA, the PKVA will have generated a different PKVN, and thus the PKVN used in the hash computation will be different. Since the hash computation uses a collision-resistant hash function, if either the public key of the PKVA or the PKVN changes, the result of the computation will have a very high probability of being different.

Please replace the paragraph beginning at page 39, line 4, with the following rewritten paragraph:

Q8

4. Registration authority 1102 creates a cryptographic hash by applying a collision-resistant hash function, such as MD5 ~~of~~ or SHA-1, to the concatenation of the regular unsigned certificate 1200, the PKVN field 802 contained in the PKVC 800 sent in step 1 of Protocol P6, and the public key of the PKVA also sent in step 1 of Protocol P6. Registration authority 1102 sends this cryptographic hash to credentials server 1103.

Please replace the paragraph beginning at page 39, line 26, with the following rewritten paragraph:

Q9

2. ~~Verifier 707~~ Credentials server 1103 validates the disposable PKVC 900 sent in step 1 of Protocol P7. ~~Verifier 707~~Credentials server 1103 uses field 903 to verify that the certificate 900 has not expired. ~~Verifier 707~~ Credentials server 1103 verifies the signature 904 using the public key of PKVA 701 also sent in step 1 of Protocol P7.

Please replace the paragraph beginning at page 40, line 14, with the following rewritten paragraph:

Q10

5. Credentials server 1103 creates, signs, and sends to subject 706 a regular disposable certificate 1300. Regular disposable certificate 1300 is illustrated in Figure ~~7~~ 19 and comprises the following fields: one or more fields 1301 containing metadata, such as serial number and issuer name; a field 1302 containing the public key of the subject 706, identical to the field 901 of the

disposable PKVC 900 sent by subject 706 in step 1 of Protocol P7; one or more fields 1303 identical to the one or more subject identity attributes 1203 of the regular unsigned certificate 1200; a field 1304 specifying an expiration date/time for the regular disposable certificate 1300; and one or more fields 1305 containing the signature of credentials server 1103 on a sequence of non-signature fields 1306. The expiration date/time specified by field 1304 must be no later than the expiration date/time specified by field 903 of the disposable PKVC 900 sent by subject 706 in step 1 of Protocol P7. If the regular unsigned certificate 1200 sent by subject 706 in step 1 of Protocol P7 contains the optional field 1205 specifying a duration for the validity interval of disposable certificates, the expiration date/time specified by field 1304 must also be no later than the end of an interval of such duration that starts when the disposable certificate 1300 is created.

Please replace the paragraph beginning at page 41, line 11, with the following rewritten paragraph:

In authentication with unsigned certificates as described in above incorporated co-pending Patent Application entitled "LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING UNSIGNED CERTIFICATES," the subject registers its public key and identity attributes with the certificate authority. The certificate authority issues an unsigned certificate to the subject, which binds the public key to the attributes, and sends the cryptographic hash of the unsigned certificate to each verifier, which stores the cryptographic ~~has~~ hash in its hash table. Later, the subject submits the unsigned certificate to a verifier and demonstrates knowledge of the private key associated with the public key contained in the certificate. The verifier computes the cryptographic hash of the unsigned certificate and checks that the computed cryptographic hash appears in its hash table.

Please replace the paragraph beginning at page 42, line 3, with the following rewritten paragraph:

Later the subject submits the regular unsigned certificate to a verifier, together with a disposable PKVC and the public key of the PKVA. The verifier checks that the disposable

PKVC has not expired and uses the public key of the PKVA to verify the signature on the disposable PKVC. If the regular unsigned certificate includes an optional field containing the subject's public key, ~~The~~ the verifier checks that the public key appearing in the regular unsigned certificate is the same public key that appears in the disposable PKVC, and the subject demonstrates knowledge of the private key associated with that public key. The verifier computes a cryptographic hash by applying the same collision-resistant hash function to the concatenation of the unsigned certificate, the PKVN contained in the PKVC, and the public key of the PKVA, and checks that the cryptographic hash appears in its hash table.

Please replace ~~the~~ paragraph beginning at page 44, line 1, with the following rewritten paragraph:

3. Certificate authority 1401 creates a regular unsigned certificate 1500, stores the regular unsigned certificate 1500 it in its database 1402, and sends the regular unsigned certificate 1500 to subject 706. Regular unsigned certificate 1500 is illustrated in Figure 21 and comprises the following fields: one or more fields 1501 containing metadata, such as serial number and issuer name; an optional field 1502 containing the public key of the subject 706; one or more fields 1503 containing the one or more identity attributes sent by subject 706 in step 1 of Protocol P8; and an optional field 1504 specifying an expiration date/time.